



**Transportation
Security
Administration**

Paul Rosenzweig
Chairperson
DHS Data Privacy and Integrity Advisory Committee
U.S. Department of Homeland Security

Dear Mr. ~~Rosenzweig~~ *Paul*:

Thank you for your July 7, 2005 letter requesting additional information about the Transportation Security Administration's (TSA) Secure Flight and Redress Programs. I have prepared responses to each of your questions below. Several of your questions pertain to the Redress Program within TSA's Office of Transportation Security Redress (OSTR). I have coordinated the responses to these questions with Virginia Skroski, the Acting Director of OSTR.

Question #1: What processes will be put in place to make certain Privacy Act compliance keeps pace with changes in the development of Secure Flight?

Your question accurately points out that Secure Flight is a dynamic and evolving program. As an example, on June 22, 2005, TSA updated its Privacy Act System of Records Notice for the Secure Flight Test Records System and the Privacy Impact Assessment for the Secure Flight test phase to reflect recent testing developments. The Secure Flight program will continue to work closely with the TSA Privacy Officer, the DHS Chief Privacy Officer, and the Office of Chief Counsel to ensure that the Secure Flight program's collection, maintenance, and disclosure of information is consistent with the Privacy Act. Protecting individuals' privacy is a top priority of Secure Flight.

Question #2: The stated reason for collecting data from commercial sources was to drive down the false positive rate. Has a full assessment been done to determine whether the rate can be driven down by other methods (e.g. allowing individuals who are falsely identified to opt-in to the sharing of an additional identifier)?

TSA has and continues to assess how best to reduce the false positive rate when matching airline passengers to the government's consolidated terrorist watch list. To date, we have examined four techniques:

- Provision of additional data elements, such as full name and date of birth, by passengers. Our testing showed a potential reduction in the false positive rate of up to 60% when passenger data records included the full name and date of birth.

- Use of commercial data elements, such as second surname, address, date of birth, and gender to enhance the passenger record. Our testing has shown a potential reduction in the false positive rate of up to 30%; we plan to do additional testing in this area.
- Use of other data elements, such as date of birth and address, already resident in the Passenger Name Record (PNR); to date, the results are inconclusive but further inquiry is planned.
- Retention of vetting history for those persons mistakenly identified as matches to the watch list to enable Secure Flight to recognize these individuals and prevent them from being flagged on future flights. This is a core aspect of all vetting at TSA and promises to be very useful in Secure Flight.

We know as well that passengers who today complete the redress process through the provision of personal information to TSA enjoy far greater convenience at the airport. We are examining, under Secure Flight, whether such individuals should be provided with a unique personal identifier that they can provide to air carriers to ensure they are not flagged as potential watch list matches.

Question #3: With respect to the matching algorithm, what steps are being taken to assess the efficacy of using private sector data? Has any independent analysis been undertaken?

As indicated above, preliminary test results have shown a potential reduction in false positive watch list matches of up to 30% by enhancing PNRs with commercial data. As will all key aspects of Secure Flight, these results are under review by MITRE, which serves as Secure Flight's provider of Independent Validation and Verification, as well as by the Government Accountability Office on behalf of Congress.

Question #4. You said in your remarks that you are establishing a "redress office to handle false positives." When will this office be operational? How will it operate?

The Office of Transportation Security Redress (OTSR) is slated to be operational in August 2005. If an individual believes that he or she has been wrongfully delayed or denied boarding based as a result of the watch list check performed as part of Secure Flight, the individual may contact OTSR to seek assistance. The individual may obtain the necessary forms and information to initiate the redress process on the TSA website or by contacting OTSR by mail. The individual must submit the requested personal information and copies of identifying documents to TSA. OTSR, in coordination with TSC and other appropriate Federal law enforcement or intelligence agencies, will review the documentation and provide the individual with a written response. TSA will then retain the information that the individual submitted to expedite the screening process for that individual during future air travel to prevent repeated delays.

Question #5. Will the operation processes and performance measures of the redress office be publicly available?

Yes.

Question #6. How are you defining “redress?” That is, is the expectation that a traveler falsely matched will be provided some form of ID that would allow them to pass future screening, assuming the algorithm continues to produce a false positive for the passenger? Or does that screening system have a provision to enter data that would preclude individuals from being identified as a suspect?

We are examining both of these options for handling misidentified individuals. TSA will retain information provided by individuals during the redress process to distinguish them from persons of interest during future travel and might provide them with a unique personal identifier that they can provide to air carriers to ensure they are not flagged as potential watch list matches.

Question #7. Would your office consider providing a notice to each passenger showing the public sources of data used for matching and how to access and amend those commercial databases?

Yes.

Question # 8. Please provide more information about the audits you conduct in your system.

Prior to the launch of Secure Flight, the program must receive official Authority to Operate (ATO) from the TSA Chief Information Officer (CIO), who makes an independent judgment as to whether the system is secure.

Security for the system includes real-time auditing of data transactions, events, and activities that are performed on or within the system. These include creation of records or accounts, and authorized or unauthorized access to the system, its sub-systems, or data for any purpose (read, modify, delete). The audit mechanism maintains individual accountability of a user’s or the system’s access to the objects that it protects.

The system also maintains a record of all policies and rules that are resident on the system and creates an audit record of any changes to a policy or rule within the system. Audit records are generated for, but not limited to, successful and unsuccessful login attempts; actions taken by authorized systems administrators; file open/close violations; unauthorized file modifications; user attempts to modify system or user parameters; and user attempts to access locked files/folders. Each audit record includes a timestamp, the date-time of the event, name of the system component on which the event occurred, type of event, subject identity, and a success or failure indication. Within DHS, security audit logs are maintained for a period of seven years.

In addition to the manual review of audit logs by security personnel, operators receive immediate notification of security audit events through the use of automated system and network management tools.

To ensure compliance with security requirements, a system security audit must be conducted annually by the Inspector General. Additionally, an annual self-audit report on each system must be submitted to the information technology security officials in accordance with NIST SP800-26.

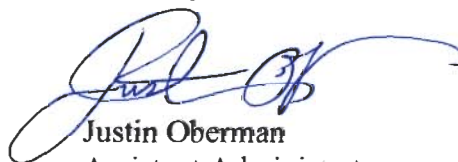
Question #9: What are the ramifications for misuse, either intentional or due to negligence? Are there any real legal consequences that hold people accountable?

There are criminal and civil penalties for unauthorized disclosure of information under the Privacy Act. Numerous steps are prevent misuse of data in the Secure Flight system. Data is maintained at a secure facility and the information is protected in accordance with rules and policies established by TSA and DHS for automated systems and hard copy storage, including password protection and secure file cabinets. Personal information is treated as Sensitive Security Information (SSI) and protected in accordance with TSA's SSI policies.

Access to personal information is limited to only those TSA employees and contractors who have a "need to know" to perform their duties associated with Secure Flight. Each employee and contractor associated with the Secure Flight program has completed privacy training. In addition, contract employees authorized to access personal data are required to sign non-disclosure agreements. If a TSA employee were to misuse passenger personal information, the employee would be subject to appropriate disciplinary action. Finally, TSA's records retention schedule will describe in detail how long data will be retained and when it will be destroyed.

I appreciate your interest and that of other members of the Committee in Secure Flight. Your participation in the development and standup of the program is beneficial to TSA and to the important security needs that the program is designed to meet. As I have said, security and privacy are the core of Secure Flight; the Committee is strongly positioned to help us achieve the former without compromising the latter. I look forward to working with you in the coming weeks and months and beyond.

Sincerely,



Justin Oberman
Assistant Administrator
Secure Flight/ Registered Traveler
Transportation Security Administration

cc: Michael P. Jackson, Deputy Secretary of Homeland Security
Kip Hawley, Assistant Secretary of Homeland Security, TSA
Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Department of Homeland Security